

PCSRF Workshop - December 2001

Application of the Common Criteria in Support of Process Control Systems Security Specification

Michael McEvilly

mam@decisive-analytics.com

703.414.5002



Overview

- Background - Establishing a foundation
 - Understanding CC Concepts & Model
- Obtaining Workshop Objectives
 - Bounding the problem
 - Issues in Defining and Scoping the Target
 - Addressing Vulnerabilities
 - Policy, Threats, Countermeasures

Importance of Fundamentals

- We solve the wrong problem
 - and wonder why solutions continue to fail
- We confuse concepts with the application of the concepts
 - and wonder why the process is so difficult

System Life-Cycle Processes

- Engineering
- Integration & Test
- Operation & Maintenance
- Retirement

System Life-Cycle Processes

Finer Granularity

- Concept Definition
- Requirements Articulation
- Design Development
- Implementation Representation
- Verification
- Operation
- Evolution
- Retirement

System Life-Cycle Processes

Common Criteria Focus

- Concept Definition
- **Requirements Articulation**
- Design Development
- Implementation Representation
- Verification
- Operation
- Evolution
- Retirement

System Life-Cycle Processes

Common Criteria Scope of Potential Impact

- Concept Definition
- Requirements Articulation
- **Design Development**
- **Implementation Representation**
- **Verification**
- **Operation**
- **Evolution**
- Retirement

Requirements are articulated through
Specification

The Specification Umbrella

Specifications



Importance of the Specification

- The specification
 - provides a means to communicate
 - establishes basis for ‘truth’ or ‘correctness’
 - often serves as a translation medium
- The specification integrity cannot be compromised
 - any process, event, activity based upon a specification is only as good as the specification

Forms of Specification

- Functional or Performance
- Safety
- Human Factors
- Security
- ConOps
- Policy

Specification Distinction Difficulties

- Capability vs. Configuration
 - what “**may**” be done vs. what “**is**” being done
 - potential vs. realization
- Capability vs. Design
 - what it must do vs. how it must do it
- Physical vs. logical
 - how I “see” it vs. how I “describe” it

Specification Correctness Concerns

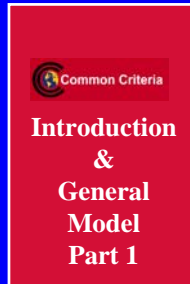
Stakeholder View

- Getting the right requirements
 - sufficiency of the solution to meet constraints of the business or mission case
 - budget
 - time
 - resources
 - technology

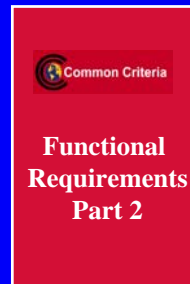
Evaluator & Stakeholder View

- Getting the requirements right
 - in compliance with standards
 - complete, consistent, coherent
 - organization, traceability
 - no redundancy, no ambiguity

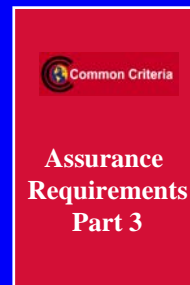
What is the CC?



Part 1 - Introduction & General Model



Part 2 - Security Functional Requirements



Part 3 - Security Assurance Requirements

What Is the CC?

*“Common Criteria for Information Technology
Security Evaluation”*

- Common Criteria

- Meta-standard of criteria and constructs used to develop security specifications

- Protection Profile (PP)
 - Security Target (ST)

... in support of the evaluation of products and systems

Common Criteria Focus

... in support of the evaluation of products and systems

- Focus of CC is evaluation
 - Part 3 defines specific requirements
 - Content and presentation of evaluation evidence
 - Verification tasks for the evaluator
 - Part 2 has no such [intentional] focus
 - Applicable in any context [supposedly]

The Common Criteria (CC)

“Common Criteria for Development of Information Technology Security Specifications”

- The CC is a meta standard that defines
 - a requirements specification framework that
 - characterizes solutions (PP)
 - defines “as built” or “as-to-be-built” solutions (ST)
 - a catalog of criteria used to populate the framework
 - Part 2 – Security Functional Requirements
 - Applicable to any “problem space”
 - Part 3 – Security Assurance Requirements
 - Applicable to any “verification space”

Requirement Specification Framework

Protection Profile & Security Target

- Context information
 - Introduction/TOE Description)
 - Application domain information
 - Secure usage assumptions
 - Organizational security policies
 - Threats
- Security Objectives
- Security Requirements
 - Functional, Assurance
- Rationale

Each as necessary to define and substantiate a security case



The Common Criteria (CC)

Functional and Assurance Criteria

- The CC is a catalog of criteria
 - Functional Requirements
 - used to specify what the system is to do
 - Assurance Requirements
 - used to specify what is done to verify that the system does exactly what it is supposed to do, and nothing else

CC Functional Criteria

- Specify the security properties of IT products and systems that address
 - Unauthorized disclosure (confidentiality, privacy)
 - Unauthorized modification (integrity)
 - Loss of use (availability)
 - Verification of identity (Identification and Authentication (I&A))
 - Accountability for operations (audit, non-repudiation)
- Provides a basis for comparison of different design or implementation solutions



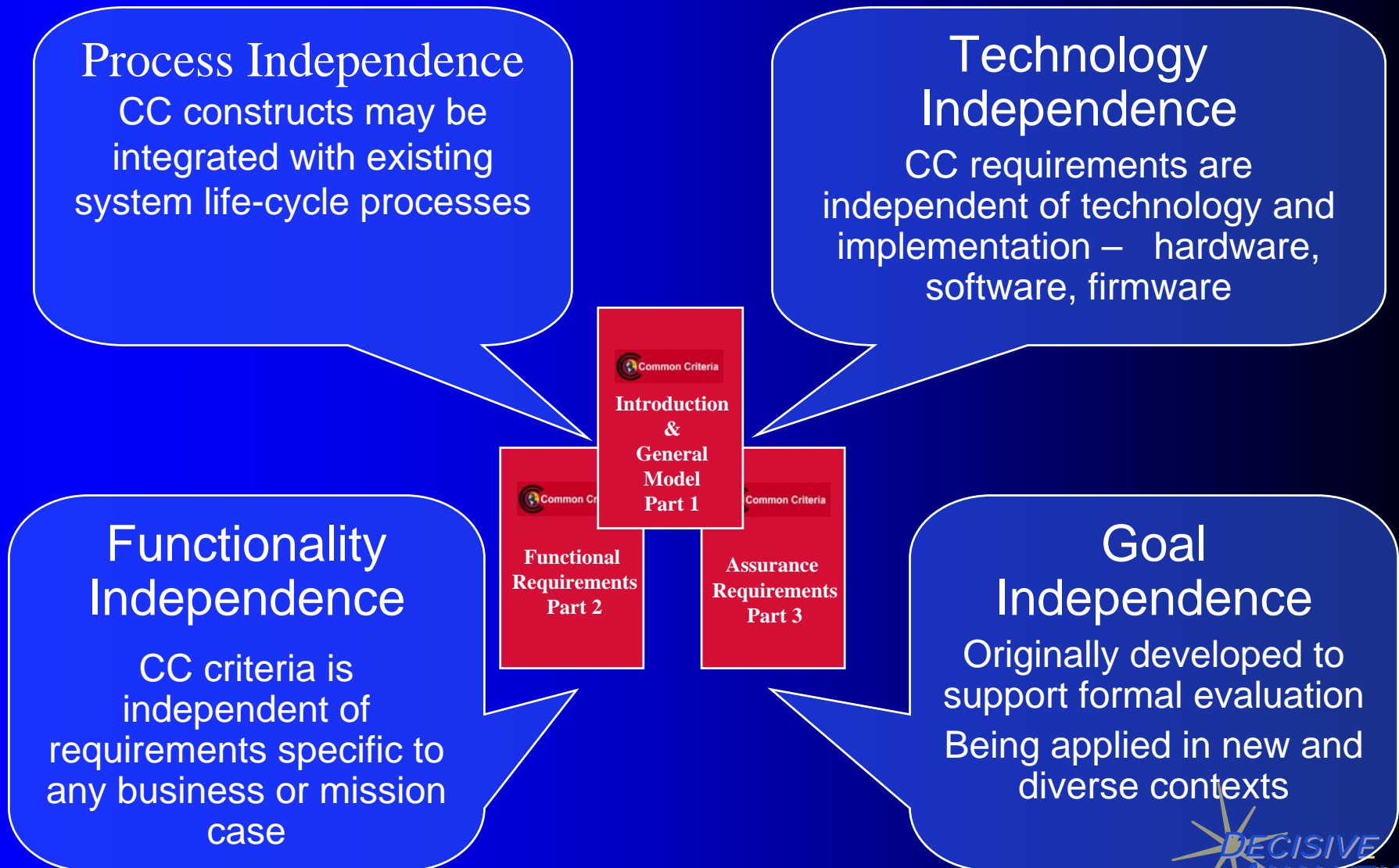
CC Assurance Criteria

- Specify the properties for verification of development life-cycle activities
- Specify the properties for verification of a continuity of knowledge as systems evolve
- Provides a basis for comparison of the results of independent evaluations

Users of the CC

- Developers of security specifications
 - Security, systems engineers
- Implementers of security specifications
 - Product and system developers, integrators
- Verifiers of the implementation of a security specification
 - Certifiers, evaluators, auditors

Application of the CC



The CC Requirements Specification Framework

Specification Philosophy
Concepts & Constructs



CC Specification Philosophy

A Requirements Engineering Approach

- Specification framework provides for
 - Specification of a security problem
 - Specification of the security solution
 - implementation
 - verification
- Information captured in various ‘constructs’
 - each presents a ‘view’ of the problem or solution
- Concepts relate information
 - within a construct or between constructs
 - based on proven engineering practices
- Has parallel with safety-critical system engineering specification and verification



CC Specification Philosophy

Construct Concepts

- Security Environment Construct
 - Defines and characterizes the security problem
 - assumptions about the operational environment
 - threats that must be countered
 - policys that must be enforced
- Security Objectives Construct
 - Characterizes the intended approach for
 - ensuring that assumptions are realized
 - eliminating, minimizing or monitoring defined threats
 - enforcing stated policy

CC Specification Philosophy

Construct Concepts

- Security Requirements Construct
 - Defines the functional or assurance requirements that implement the defined objectives
 - Functional requirements implement the solution
 - Assurance requirements verify the implementation

CC Specification Philosophy

Construct Concepts

- Rationale Construct

- Objectives

- argument that objectives provide 100% coverage and are suitable to meet the security environment issues

- Requirements

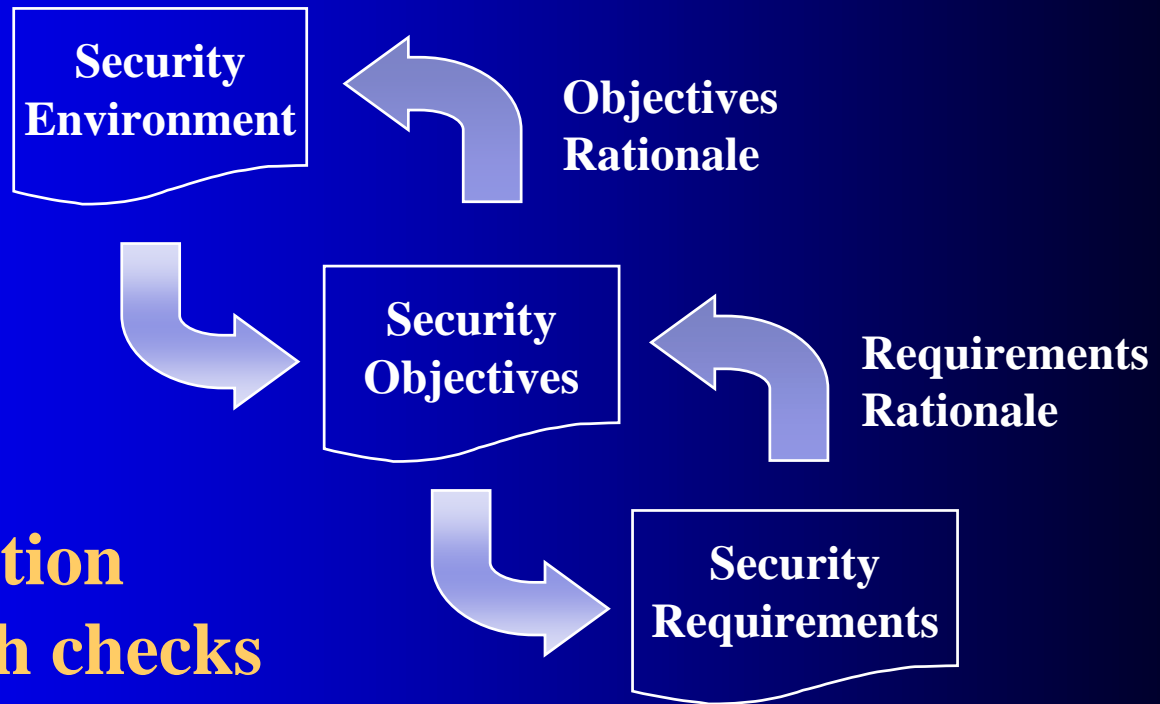
- argument that requirements provide 100% coverage and are suitable to meet the objectives

- TOE Summary Specification

- argument that security functions and assurance measures provide 100% coverage and are suitable to meet the requirements

CC Specification Philosophy

Construct Concepts



A specification framework with checks and balances to provide end-to-end correctness

CC Concept Definitions

- Target of Evaluation (TOE)
 - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation
- TOE Security Functions (TSF)
 - The parts of the TOE implementation that are relied upon for the correct enforcement of the TOE Security Policy (TSP)

CC Concept Definitions

- TOE Security Policy (TSP)
 - Set of rules that define how assets are managed, protected and distributed by the TOE
- TSF Interfaces (TSFI)
 - Interfaces to the TOE security functions
 - internal to the TOE
 - between the TOE and users and trusted products

CC Concept Definitions

- IT Environment
 - IT products or systems that are not part of the TOE but with which the TOE shares a trusted relationship
 - Trust relationship – mutual authentication of communication participants and secure methods to transfer information
- Non-IT Environment
 - The physical aspects of the world in which the TOE is placed and operates

Illustration TOE, TSF, TSFI

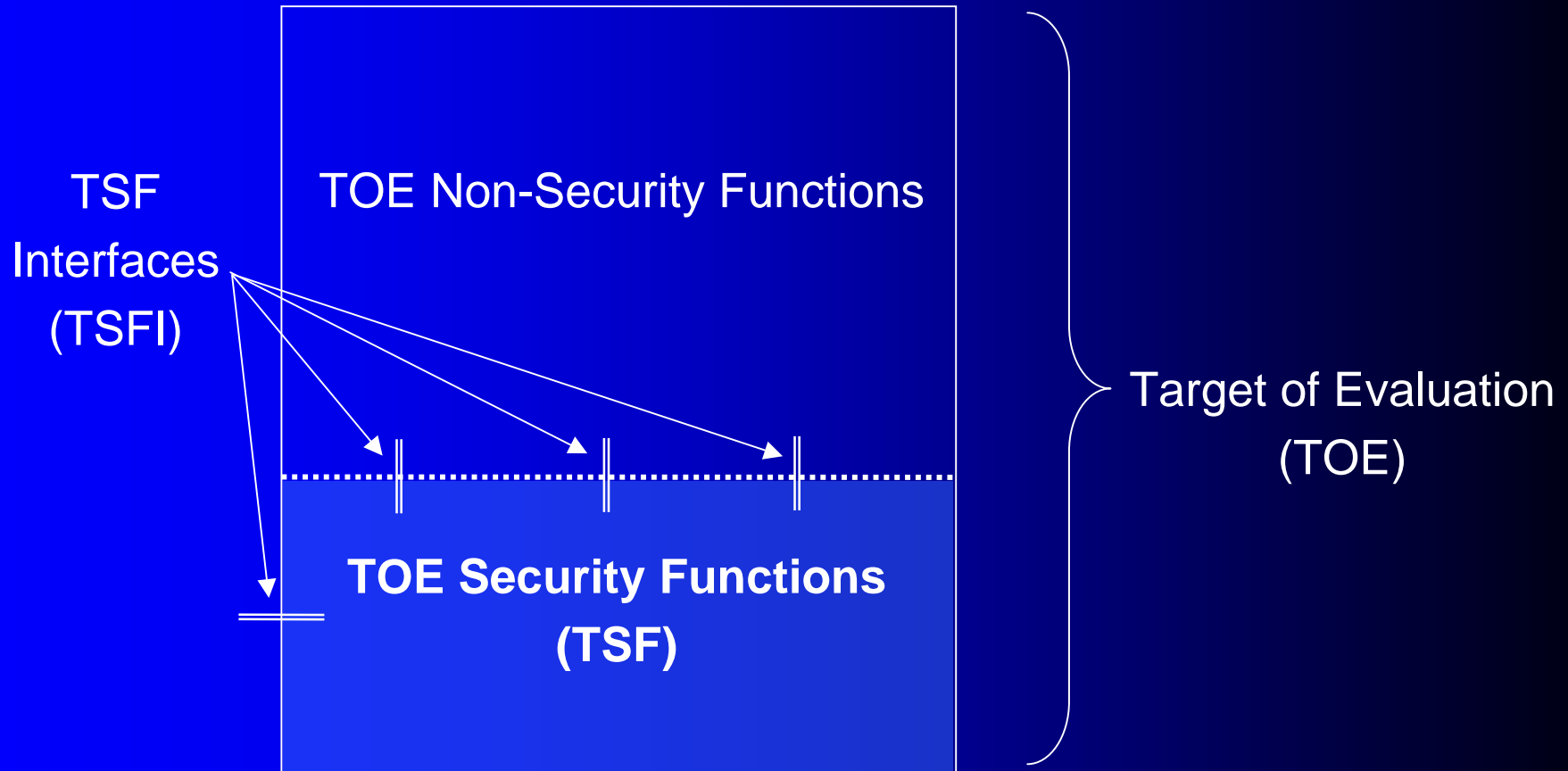
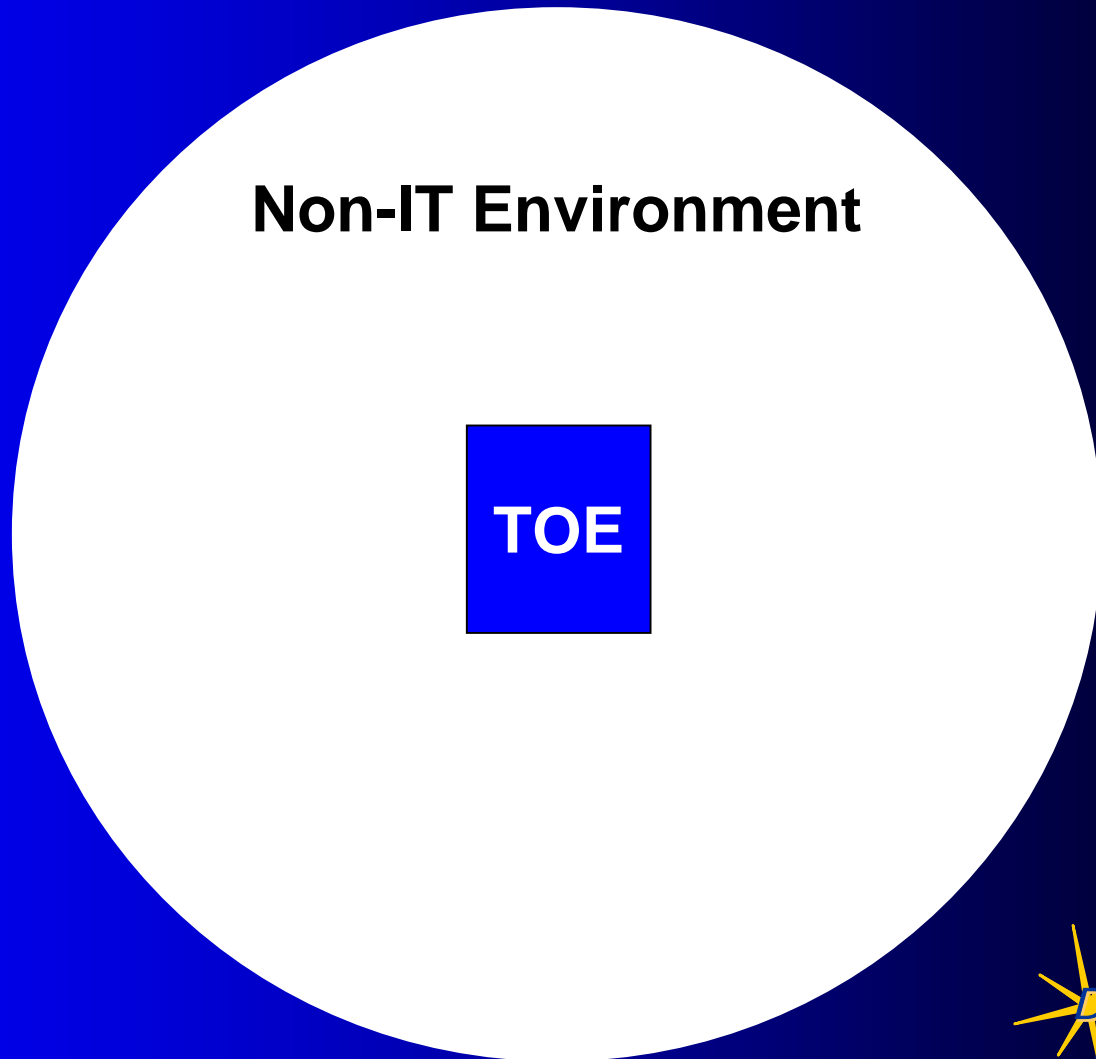


Illustration Non-IT Environment

Non-IT environment consists of the physical aspects of the world in which the TOE is placed and operates.



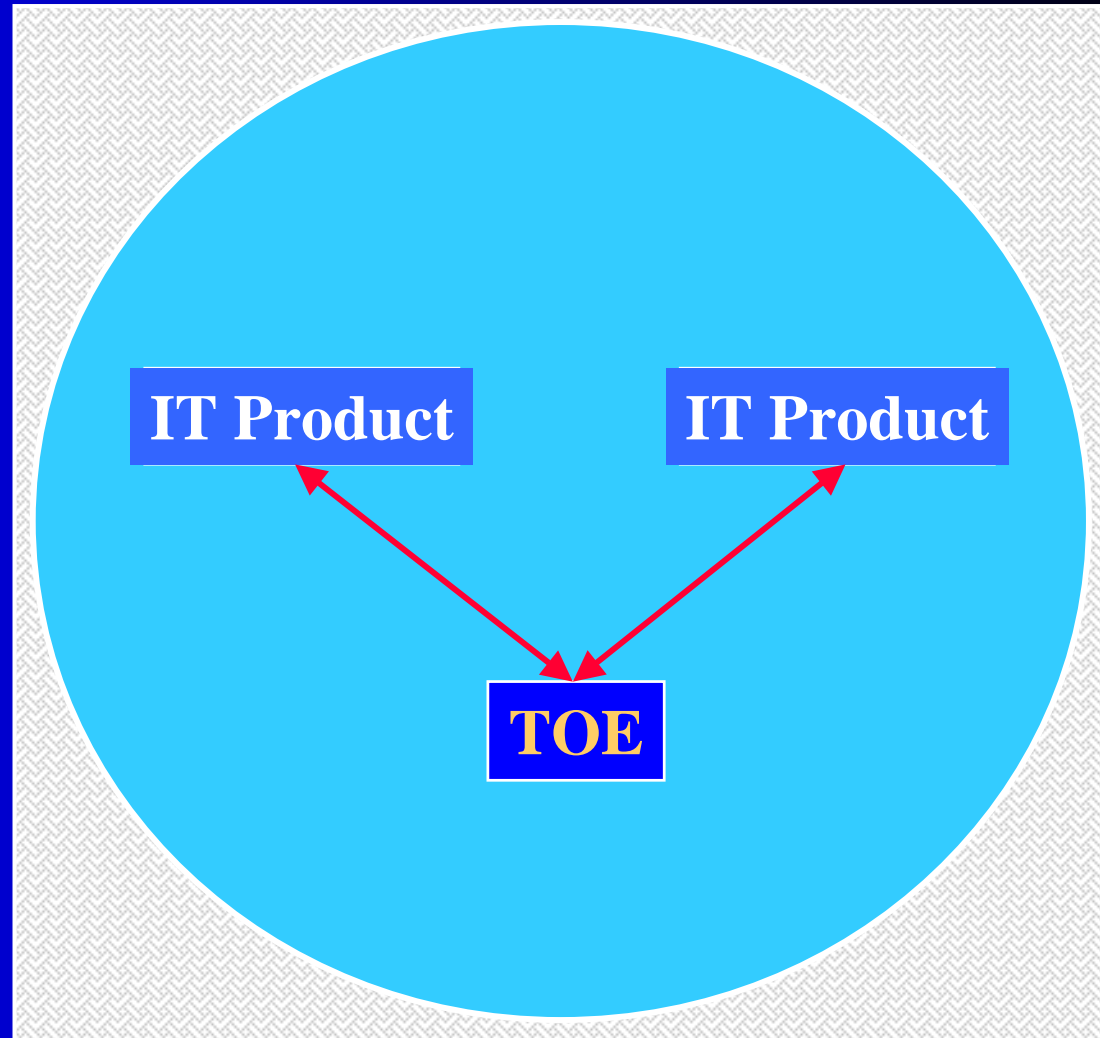
IT Environment Concept

The general environment is enclosed inside the square, i.e., the 'world'

- TOE Environment is enclosed inside the circle

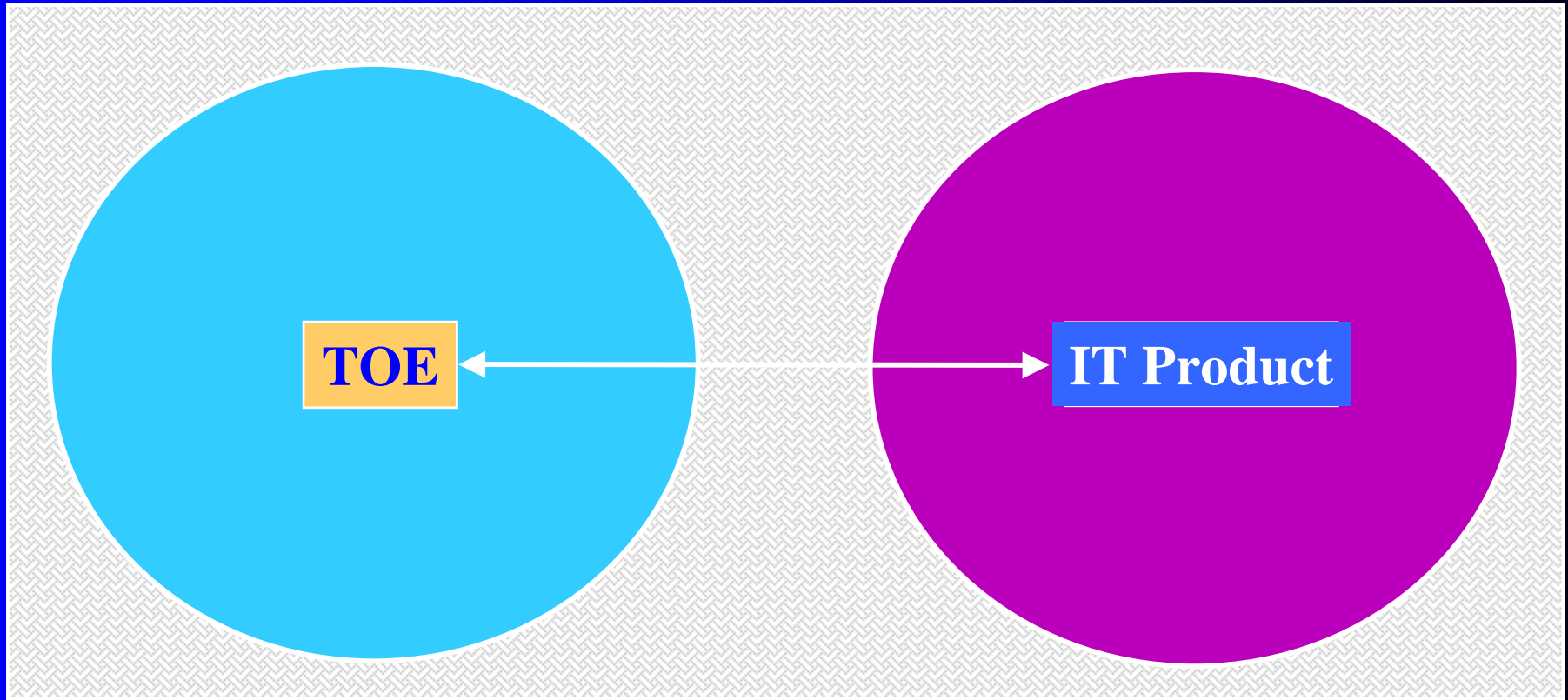
Non-IT environment implemented by the physical world

IT Environment implemented by IT capabilities



IT Environment Concept

Web Server (TOE) - Certificate Server (IT Environment)



 Non-IT environment of the Web Server (TOE)

 Non-IT environment of the Certificate Server (IT environment of the TOE)

Requirements Specification Framework Construct

The Protection Profile



What's in a PP?

- Protection Profiles are Security Specifications that include, in addition to Functional and Assurance Requirements, the following information ...
 - Context information
 - Introduction/TOE Description)
 - Environment information
 - Assumptions, Threats, Policies
 - Statement of goals (Objectives)
 - Rationale

Protection Profiles

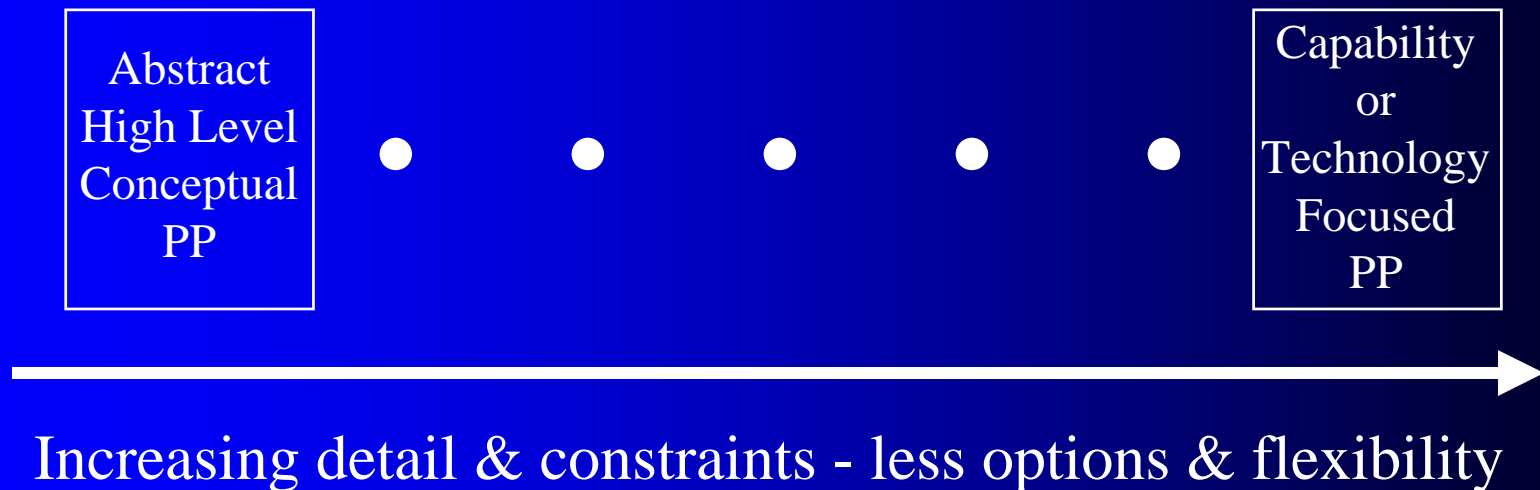
- Answers the question:
“What do I need in a security solution?”
- Characterizes the solutions space for a class of components, products or systems
- Protection Profile authors:
 - anyone who wants to state IT security needs (e.g., commercial consumer, consumer groups)
 - anyone who supplies products which support IT security needs
 - anyone ...

Purpose of the PP

- To provide a means for statement of security requirement needs
 - for acquisition
 - for development
 - for certification & accreditation
 - for any unique security documentation requirement
- PPs establish ...
 - a basis for ST development
 - a common reference for ST comparison and assessment

Protection Profile Granularity

- Requirement detail granularity is the discretion of the PP author



Flexibility in the use of PPs

- The CC defines a framework that establishes
 - correctness of a PP
 - correctness of a ST
 - the optional relationship between a PP and a ST
- The CC encourages that the PP Introduction include a reference to related PPs
 - the CC does not define what the relationship is
- Creative use of the PP concept can improve specification and acquisition processes

CC Philosophy For PP Content

- Threats/Policies are stated
 - based upon identified vulnerabilities
- Security Objectives stated
 - to counter the threats and enforce policies
- Explicit measures are adopted that
 - eliminate vulnerabilities
 - minimize vulnerabilities
 - monitor vulnerabilities

The CC and System Specification

Issues & Considerations
for the PCSRF



System Specification Issues

Scope

Interfaces

Composition

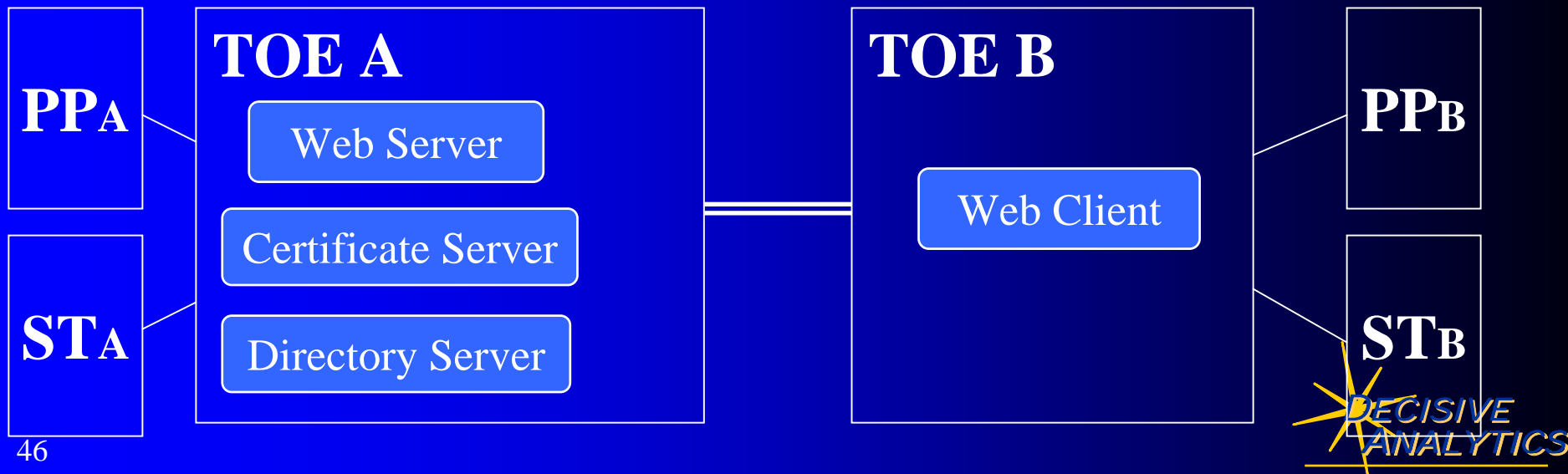
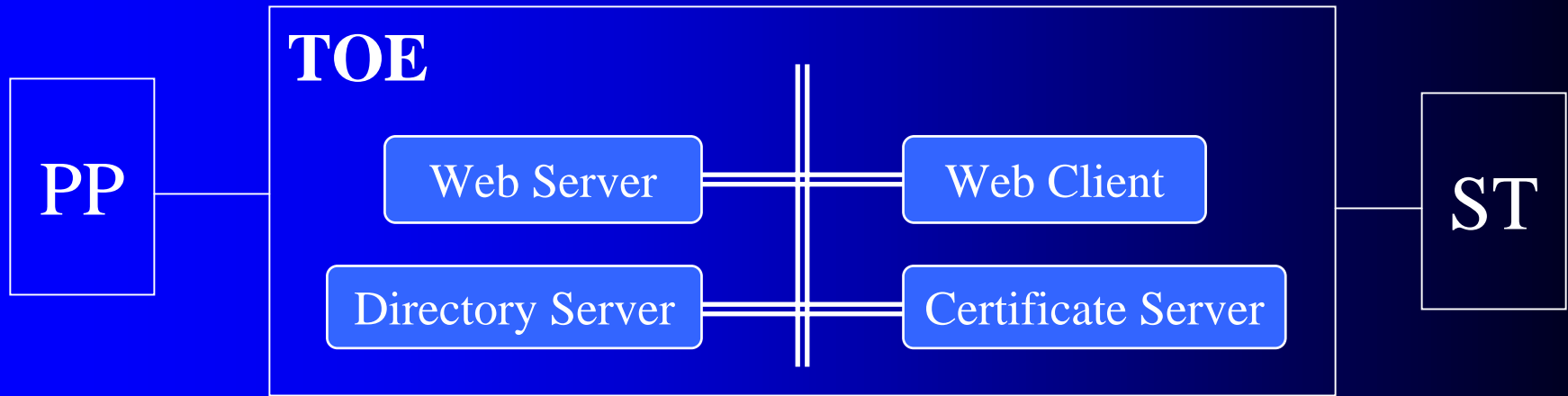
Decomposition

Trust Relationships



- Systems present unique scoping issues
 - technical
 - interfaces, scalability, composition/decomposition
 - management
 - schedule, budget, resources
- Once defined, the system is treated as a single component TOE
 - implications must be fully understood

Scope Illustration



Composing/Decomposing

Correctness of the Specification

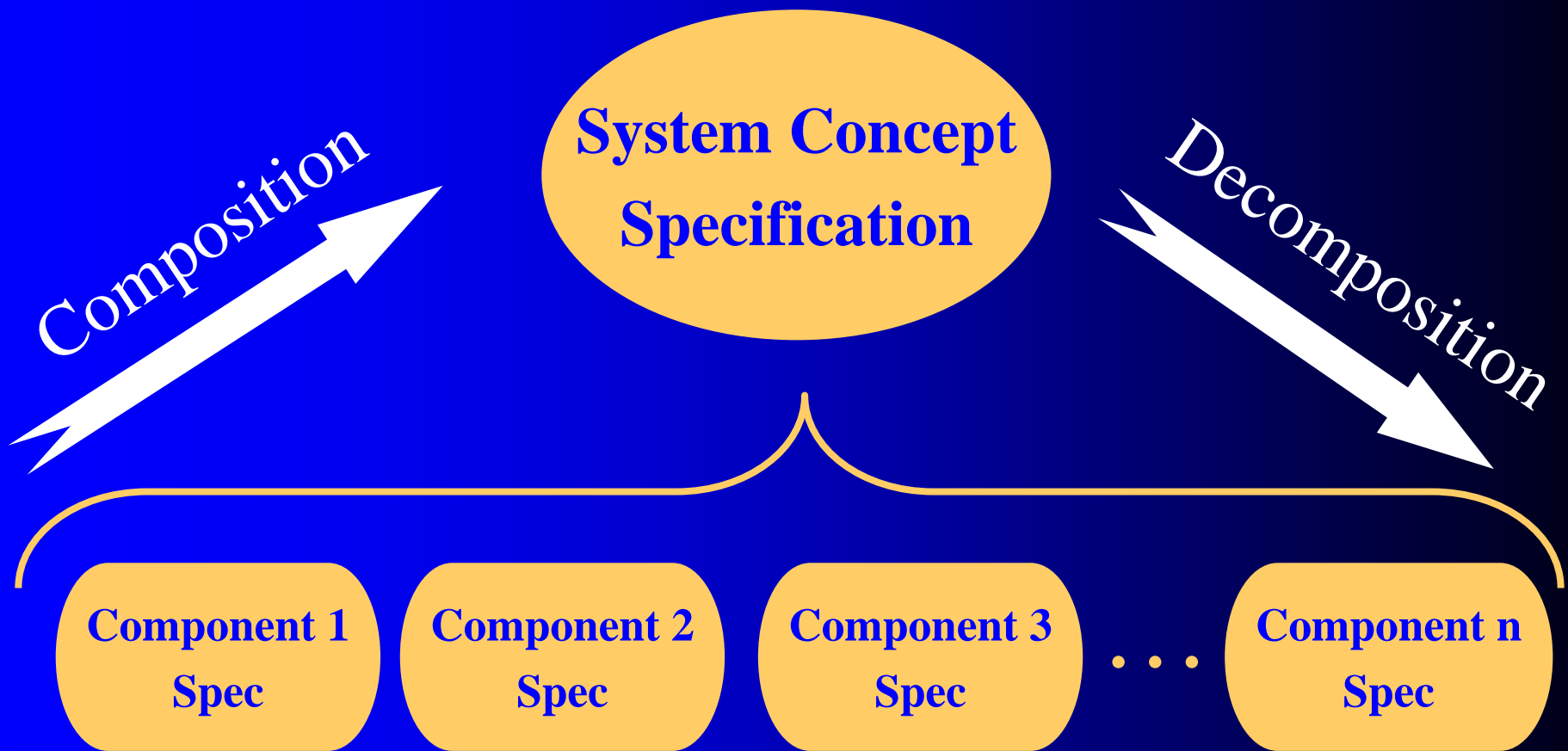
- Decomposition

- how to decompose a system concept into implementation and specification components
 - physical and logical

- Composition

- how to compose a system using pre-existing components and component specifications
 - physical and logical

Composition and Decomposition Illustration



Interfaces

- Rules for interaction between components
- Typically specified independent of functionality
 - message interface
 - programming interface (API)
 - services interface
 - plug-in interface
- May be internal or external

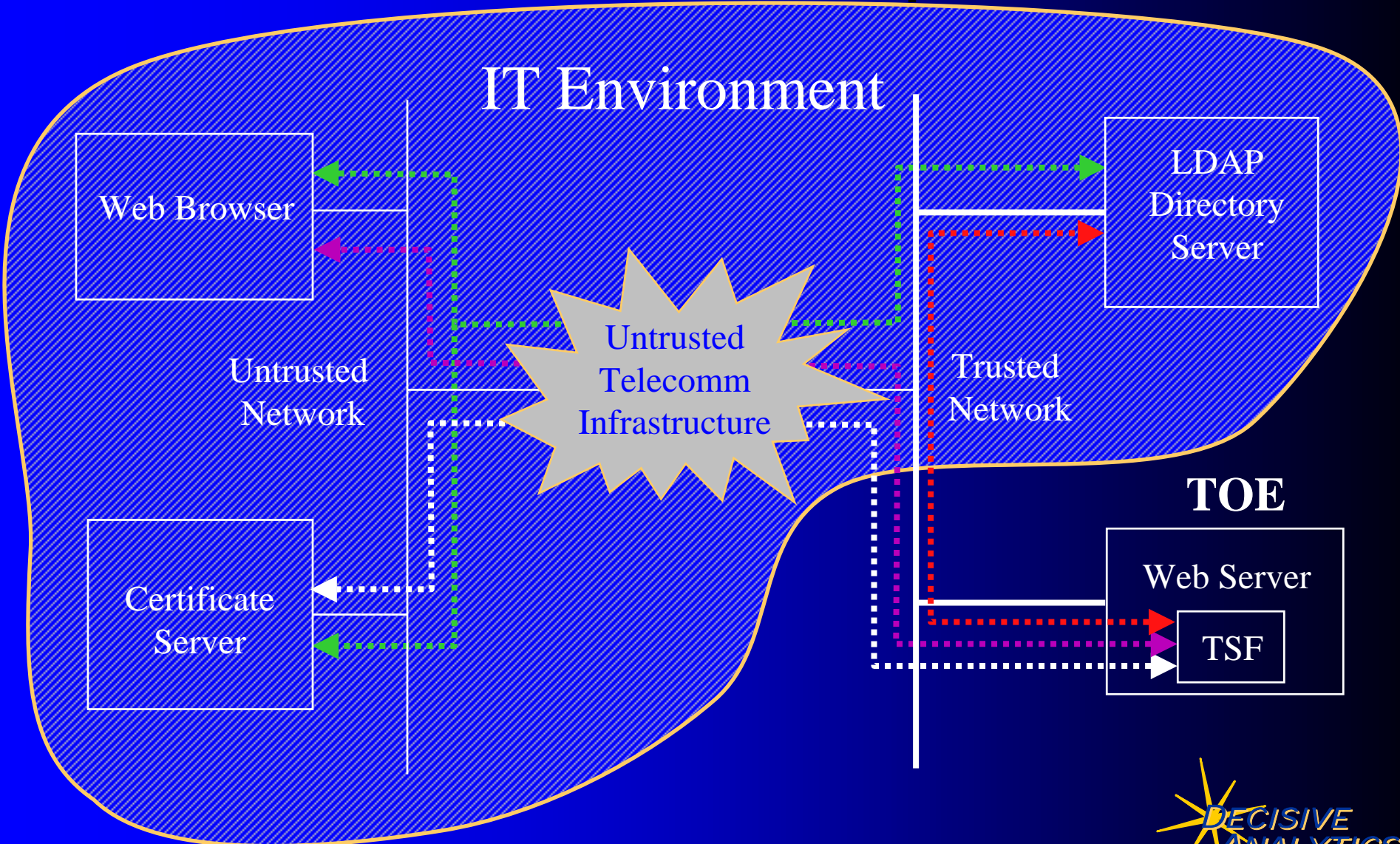
Trust Relationships

- Rules for secure interaction between components
 - special form of interface
 - subset of interface specification
- From the CC perspective
 - internal to the TOE
 - between the TOE and a remote trusted component
 - IT environment

Establishing Trust Relationships

- Trusted channels provide mechanism for trust relationships between components
 - authentication of endpoints
 - secure communication protocol
 - integrity, confidentiality, recovery
- Trusted channels provide mechanism for trust relationship between user and system
 - built on trusted channels

Trust Relationship Illustration



IT Environment

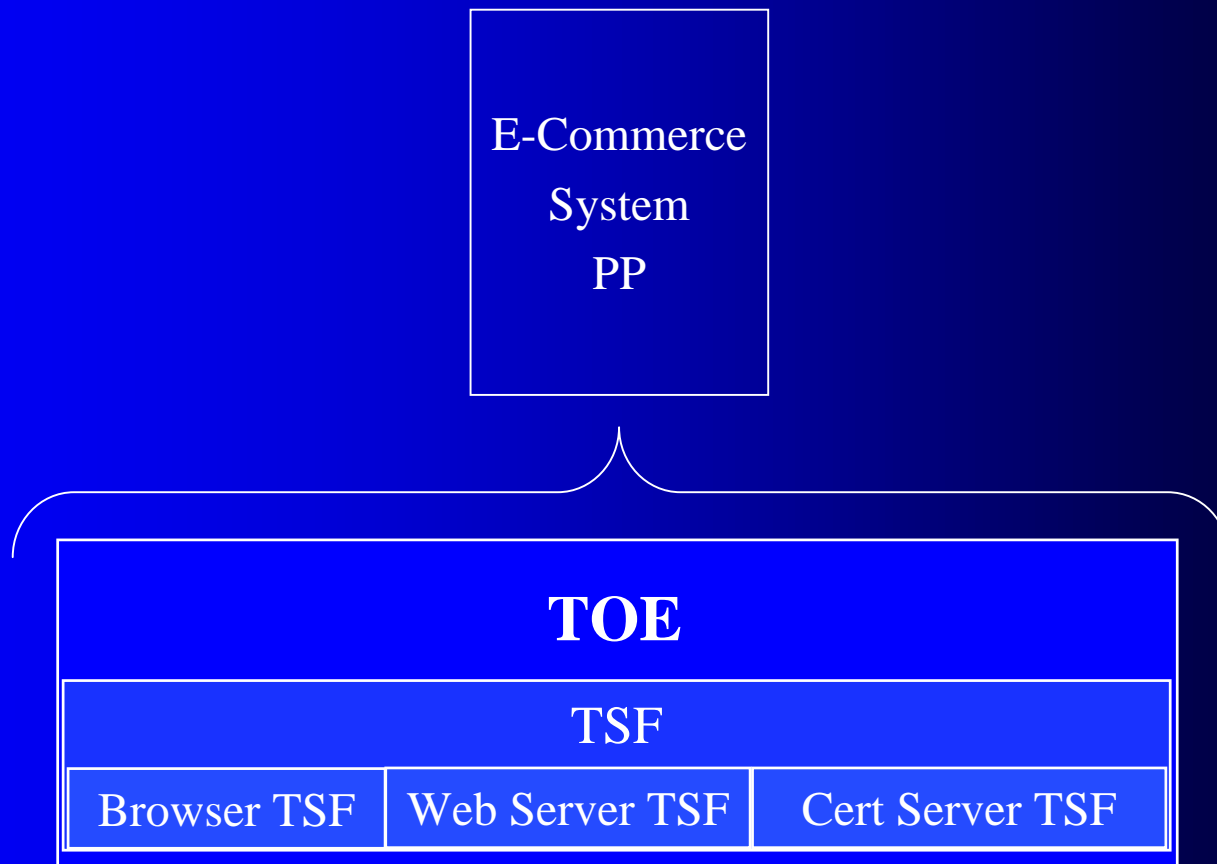
Specification of Trust Relationship with Remote Systems

- IT Environment is comprised of
 - IT components that are not part of the TOE but with which the TOE shares a trust relationship
- PP/ST has section dedicated to specification of IT Environment interfaces

System Specification Using Single Protection Profile

- Practicality dependent upon size and complexity of the TOE
- May present configuration management problems
- Organization of information important
 - by TOE component
 - by criteria
- Useful for either composition or decomposition approach

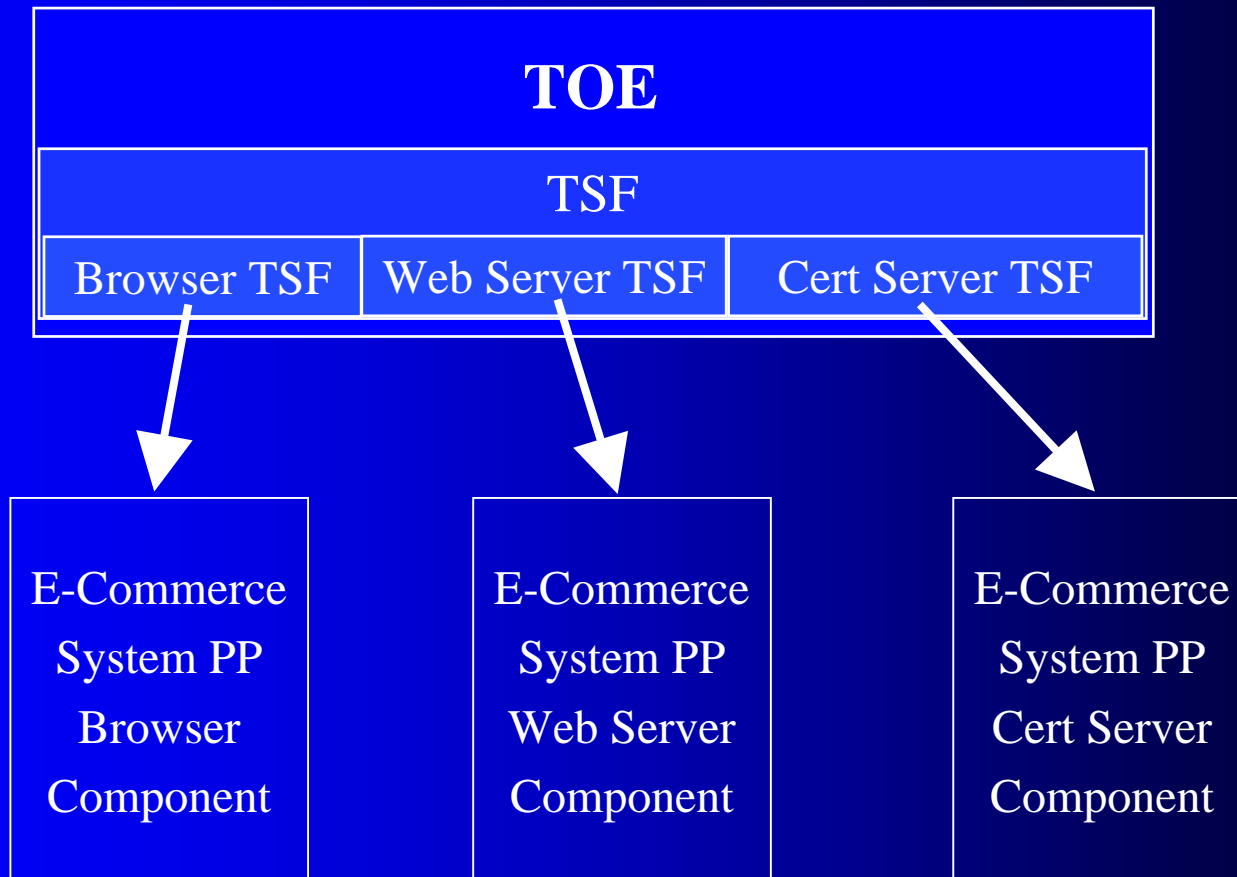
System Specification Using Single Protection Profile



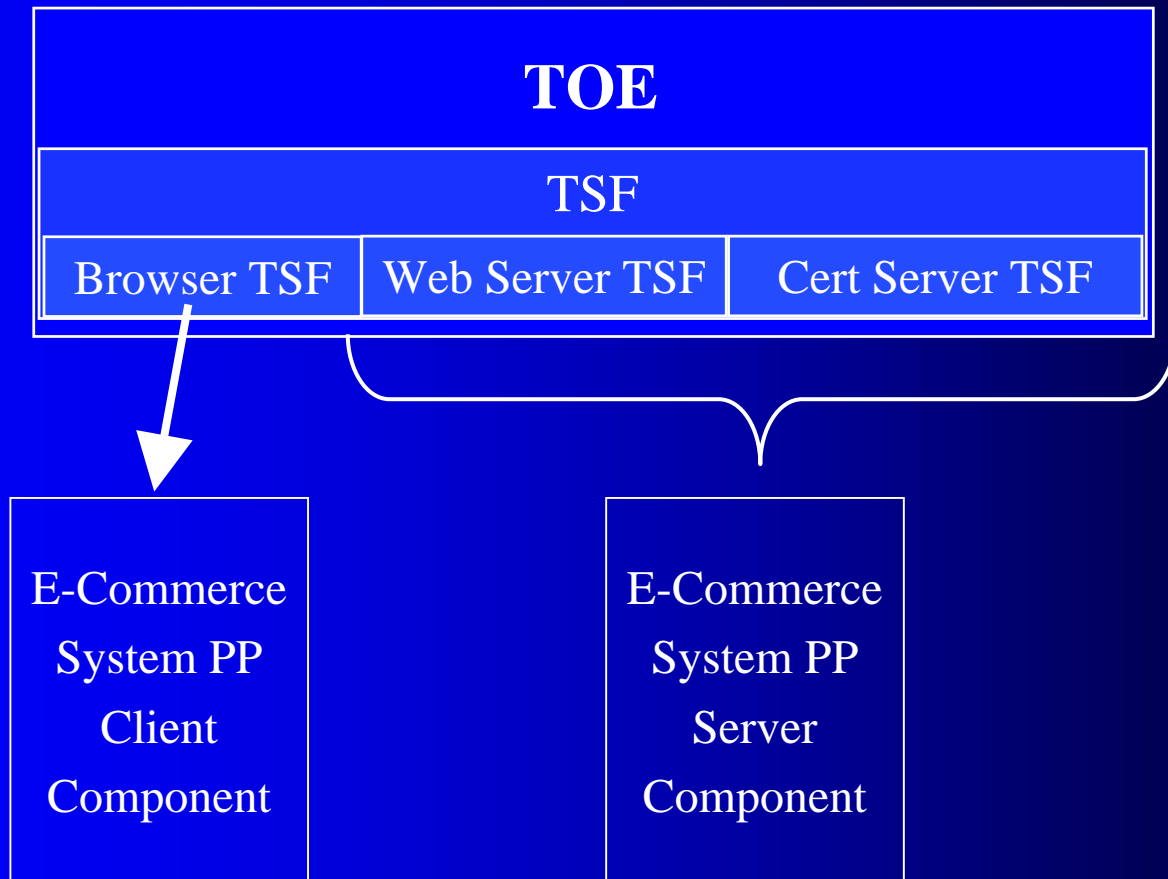
System Specification Using Multiple Protection Profiles

- May serve either purpose
 - Decomposes system into component parts
 - Compose a system from existing component parts
- Distributes workload and may map better to life-cycle processes and constraints
- Adds complexity to configuration management
 - Coordination of distinct parts
- Organization is typically by component or subsystem
- More appropriate for a composition approach

System Specification Using Multiple Protection Profiles



System Specification Using Multiple Protection Profiles



Multiple PP Approach Issues

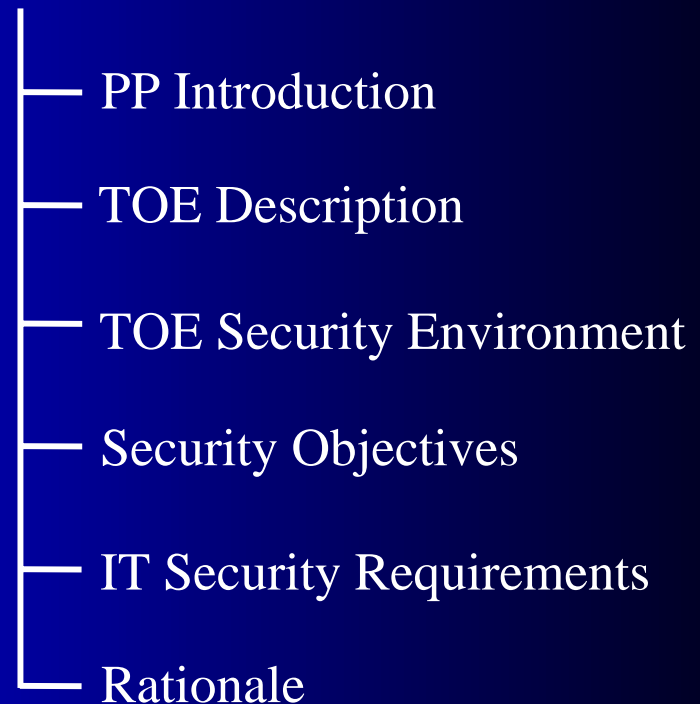
- Each PP is a standalone document
 - necessary to meet APE criteria
- No central location for discussion of the TOE as a whole system
- Difficult to understand the logical relationships

System Specification

Concept of Intermediate PP Structures

- Intermediate PP structures provide a decomposition of the specification space
- Useful where implementation options vary based upon
 - technology
 - environment
 - operational practices
 - ... and, any solution must be compliant with defined criteria
- Structure defined by variance in specification requirements
 - organized as a tree structure

Protection Profile



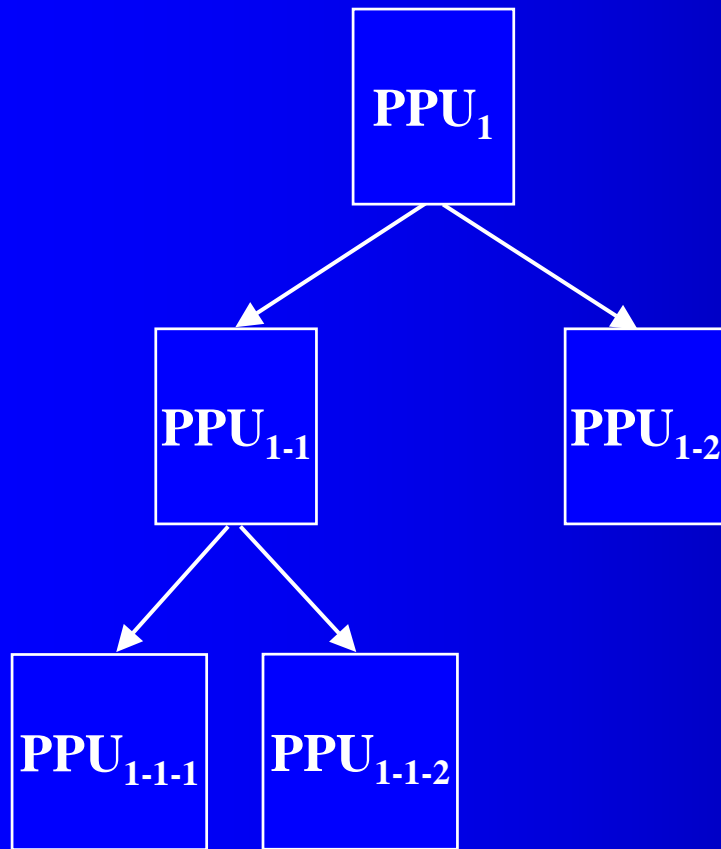
System Specification

Defining Intermediate PP Structures

- Root of tree provides mandatory information
 - TOE description
 - Security environment
 - guidance assumptions, policy mandates, threat characterization
 - Security objectives and requirements
 - for mandatory implementation approach
 - Rationale
- Root descendants elaborate or append to material at parent nodes
- Guidance is provided on application and use of PP structures

System Specification

Concept for Using PP-Like Structures



- Separate PP construct into series of specification units
- Establish relationship between units to address issues specific to the unit
- Generate a 'complete' PP by extracting units along a path of the tree

$$\text{PP} = \text{PPU}_1 + \text{PPU}_{1-1} + \text{PPU}_{1-1-2}$$



The PP Development Process

In Preparation for Development of
PCS Protection Profiles



Critical Issues

- Scope and bounding the problem
- Method of requirements articulation
- Vulnerabilities and the security environment
 - Assumptions
 - Mandatory Policy
 - Threats
- The Game Plan

Scope and Bounding

- What is the TOE?
- What is the TOE environment?
- What is the IT Environment of the TOE?

Articulation of Requirements

- Single Protection Profile
- Multiple Profiles
- Profile-like constructs

Vulnerabilities and the Security Environment

What is Assurance?

- Dictionary Definition: *conveys confidence*
- Common Criteria Definition: *grounds for confidence that an IT product or system meets its security objectives.*
- Assurance measures
 - provide a basis for a security argument
 - do not add functionality to the TOE

Basis for Assurance

- Vulnerabilities that arise from
 - Requirements
 - Incorrect, insufficient, ineffective
 - Design and Implementation
 - Incorrect design decisions
 - Errors in implementation
 - Operational Controls
 - Inadequate or overly complicated
 - Poorly documented

How Is Assurance Obtained?

- Verification and Validation (V&V)
 - by the developing organization
 - through an independent agent (IV&V)
- Verification
 - ensuring the implementation meets the stated requirements (TOE Evaluation)
- Validation
 - ensuring the requirements represent an acceptable description of the desired implementation

Dealing with Vulnerabilities

- Vulnerabilities are the basis for both threat and policy statements
- Policy statements may also reflect business case rules
 - basis for policy often to prevent
 - going to jail
 - being sued

Threats vs. Policy

- In CC model - they are equivalent
 - achieve the same end result
- Practically
 - threats are more explicit, detailed and refined
 - drive a specific functional capability or assurance need
 - policies are more broad and generic in scope
 - establish boundaries within which subordinates may operate
- Assumptions bound the scope of threats and policy

Practical CC Application

Strategy and Process

- Strategy

- What are the objectives to be met?
- How will the document be used?
- Who are the users of the developed documents?
- What information must be captured?

- Process

- Define management, development, configuration control and approval participants
- Develop procedures

Practical CC Application

Managing PP/ST Development

- PP/ST development is an engineering activity
- Disciplined application of the CC is a necessity
 - flexibility
 - varying application contexts
 - addressing CC deficiencies
- Both technical and process efforts

Practical CC Application

Managing PP/ST Development

- Process - defining the work
 - Development approach
 - Evaluation, vetting
 - Evolution
- Technical - doing the work
 - Vulnerability assessment
 - Requirements analysis
 - Writing of PP/ST sections

Practical CC Application

Managing PP/ST Development

- Accurately state requirements
 - Scope and detail
 - Consistency and coherency
 - Precision and accuracy
 - Structure and organization
- Balance “what” and “how” in response to purpose
 - Requirements abstraction
 - Physical vs. logical views and perspectives



Practical CC Application

Supporting Design & Development

- PP/ST Specification framework provides excellent basis for documentation of information design and development information
 - security environment establishes basis for requirements
 - rationale substantiates effectiveness of requirements
 - assurance requirements guide effort to document design and verify correctness of implementation



Questions

Contact Information

Michael McEvilly

DECISIVE ANALYTICS

Corporation

mam@decisive-analytics.com

703.414.5002

www.commoncriteria.com

